

A Brain-Friendly Guide

Head First CVE

Ken Lee @echain

+ Who is Ken?

- * Former Product Developer
- * Chief Security Officer (WIP)
- * Head of Synology SIRT

Synology PSIRT

The Synology Product Security Incident Response Team (PSIRT) is responsible for reacting to Synology product security incidents. The PSIRT manages the receipt, investigation, coordination, and public reporting of security vulnerability information regarding Synology products.



+ 2013 The Phantom Menace

- * Started working in 2013/01
- * No developer to respond to vulnerabilities
- * Lacked a sense of cybersecurity
- * High-profile CVEs were notified by customers

+ 2014 Revenge of the Sith

- * Severely affected by you-know-who
- * Built a working group for cybersecurity
- * Deployed security mitigations to DSM 5
- * Built private Bounty Program

+ 2016 The Empire Strikes Back

- * Built Vulnerability Response Program
- * Built invitation-only Bounty Program
- * Reported critical flaws of Photo Station
- * Disclosed vulnerabilities w/o confirmation

+ 2017 Return of the Jedi

- * Authorized as the CNA
- * Built Incident Response Program
- * Announced Security Bug Bounty Program
- * Built Product Security Assurance Program

+ Agenda

- * 00 | Common Vulnerabilities and Exposures
- * 01 | CVE Numbering Authority
- * 10 | Phrasing and Counting Rules
- * **11 | Tool for dummies**

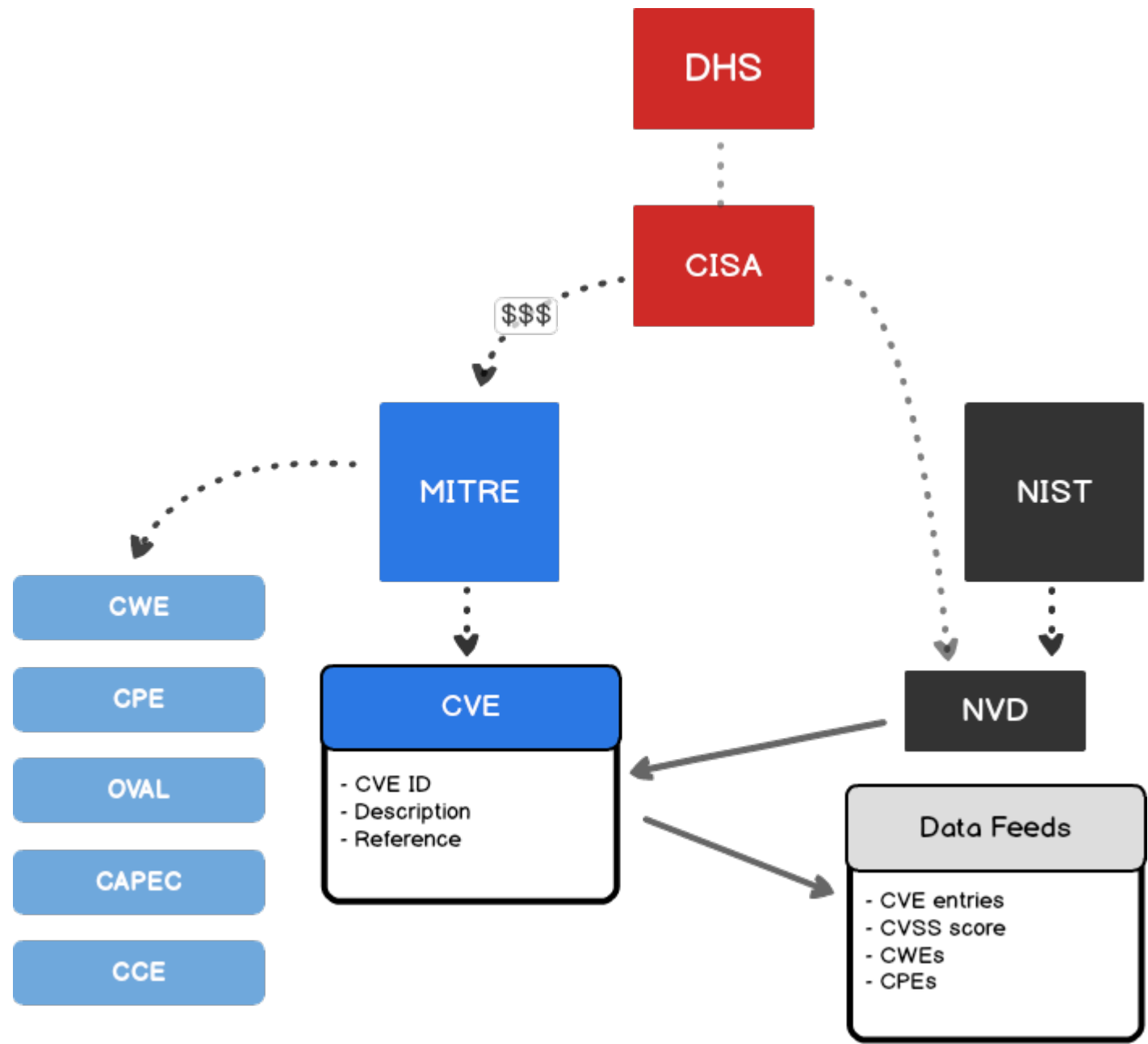
Common Vulnerabilities and Exposures

A community-driven open data registry of cybersecurity vulnerabilities



International participation



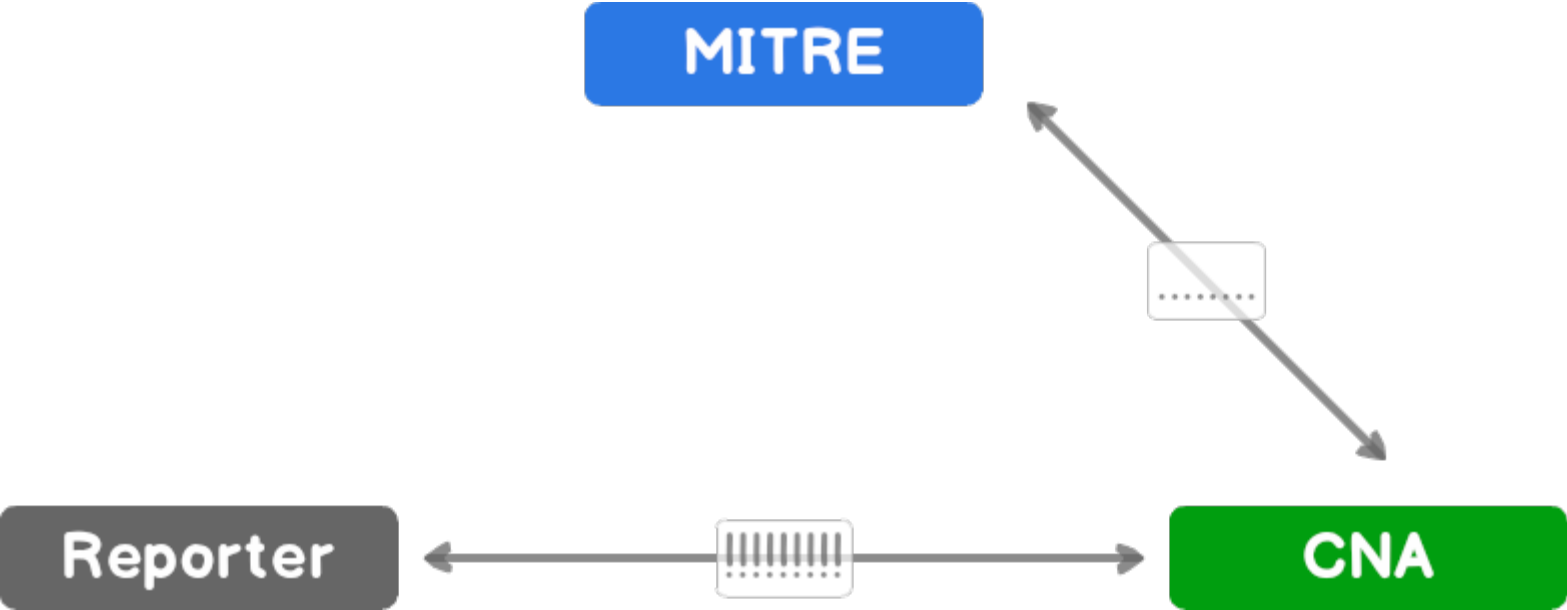


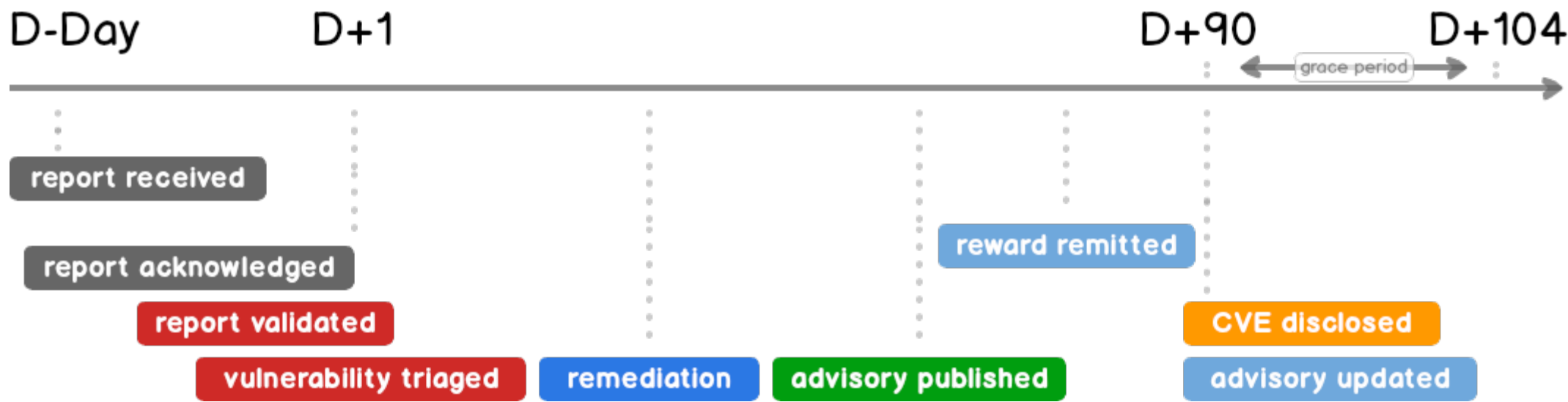
Thank you,
CNAs!

Synology Inc.









Synology-SA-19:21 #2014

Edit

Merged cve-team merged 1 commit into CVEProject:master from echain:Synology-SA-19_21 on May 9

Conversation 0 Commits 1 Checks 0 Files changed 1 +69 -7



echain commented on May 9 Contributor + 😊 ...
Added CVE-2019-11820.

Synology-SA-19:21 Verified d435bc1

echain requested a review from cve-team as a code owner on May 9

cve-team self-assigned this on May 9

cve-team added the accepted label on May 9

cve-team merged commit 8a7345d into CVEProject:master on May 9 Revert

echain deleted the echain:Synology-SA-19_21 branch on May 9 Restore branch

Reviewers

cve-team

Assignees

cve-team

Labels

accepted

Projects

None yet

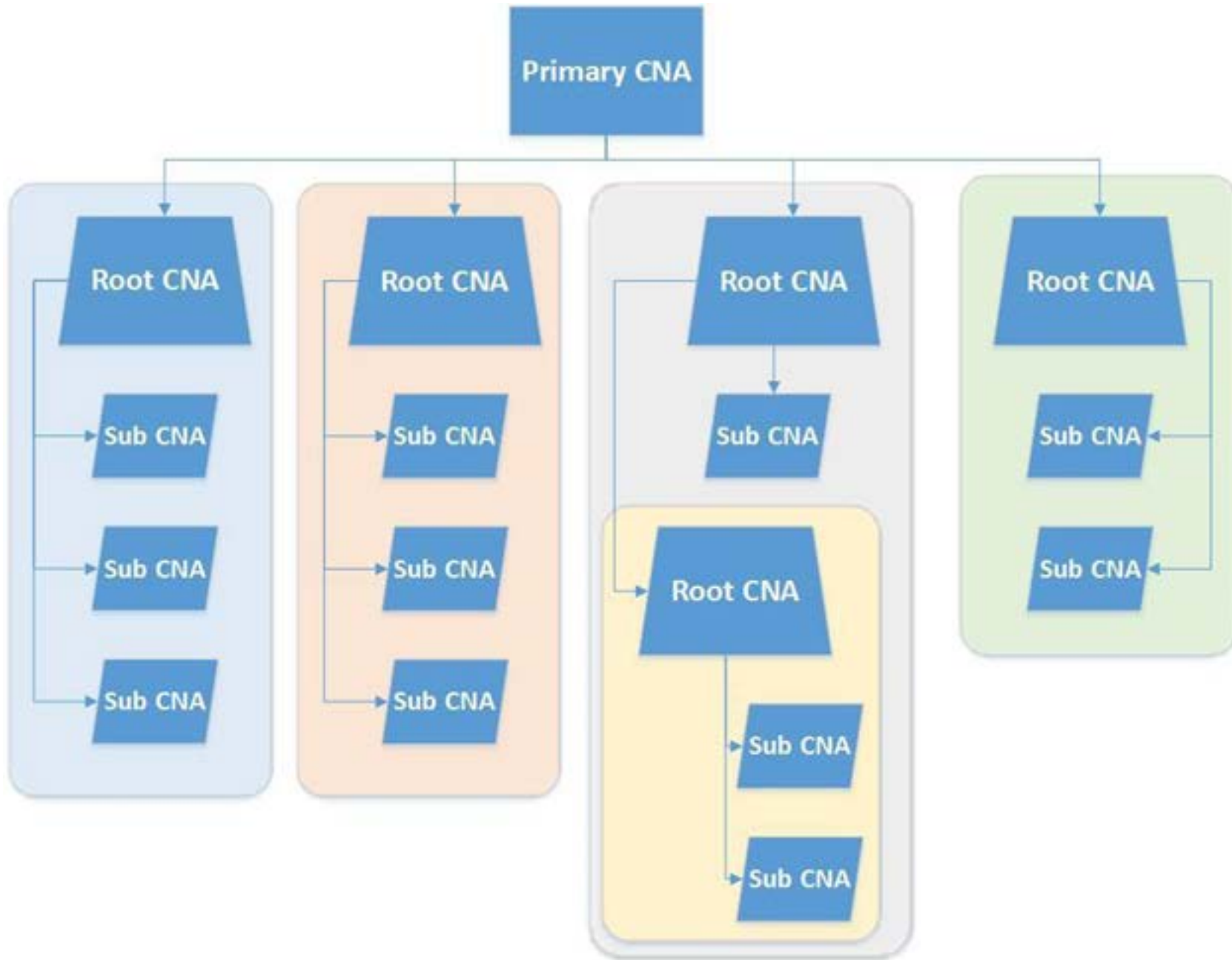
Milestone

No milestone

Notifications Customize

Unsubscribe

You're receiving notifications because you authored the thread



1. CVE ID Block Requested

At the beginning of the year, or when they use up their previous block during the year:

- Sub-CNAs request a block of CVE IDs from their Root CNA
- Root CNAs request a block of CVE IDs from the Primary CNA

2. CVE IDs Reserved

- Root CNAs provide a block of CVE IDs to their Sub-CNAs and marks those CVE IDs as reserved
- The Primary CNA provides a block of CVE IDs to the Root CNAs and marks those CVE IDs as reserved

3. CVE ID Assigned

- Sub-CNAs assign CVE IDs out of their block to vulnerabilities identified in their product(s)
- Root CNAs assign CVE IDs out of their block to vulnerabilities identified in their product(s)

4. Root and Primary CNA Notified

- Sub-CNAs provide their Root CNA with CVE ID information when vulnerabilities are made public
- Root CNAs provide the Primary CNA with CVE ID information when their, or their Sub CNA's, vulnerabilities are made public

5. CVE Published

- The Primary CNA publishes the CVE ID in the CVE List
- Sub-CNAs notify their Root CNA with any updates to their CVE IDs
- Root CNAs notify the Primary CNA with any updates to their or their Subs' CVE IDs

[CWE] in [CPE] allows
[ATTACKER] to have IMPACT
via [CAPEC].

+ MITRE's Template

- * [VULNTYPE] in [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] allows [ATTACKER] to [IMPACT] via [VECTOR].
- * [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] [ROOT CAUSE], which allows [ATTACKER] to [IMPACT] via [VECTOR].

About CWE

Overview - What Is CWE?

Targeted to developers and security practitioners, the Common Weakness Enumeration (CWE) is a formal list of software weakness types created to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code.
- Serve as a standard measuring stick for software security tools targeting these weaknesses.
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts.

[BACK TO TOP](#)

Introduction

Organizations want assurance that the software products they acquire and develop are free of known types of security flaws. Today, high-quality tools and services for finding security flaws and weaknesses in code are new and the question of which tool/service is appropriate/better for a particular job is hard to answer given the lack of structure and definition in the code assessment industry. CWE was created specifically to address these problems.

MITRE began working on the issue of categorizing software weaknesses as early 1999 when it launched the [CVE List](#). As part of the development of CVE MITRE's CVE Team developed a preliminary classification and categorization of vulnerabilities, attacks

Some Common Types of Software Weaknesses:

- Buffer Overflows, Format Strings, Etc.
- Structure and Validity Problems
- Common Special Element Manipulations
- Channel and Path Errors
- Handler Errors
- User Interface Errors
- Pathname Traversal and Equivalence Errors
- Authentication Errors
- Resource Management Errors
- Insufficient Verification of Data
- Code Evaluation and Injection
- Randomness and Predictability

CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Weakness ID: 78

Abstraction: Base

Structure: Simple

Status: Stable

Presentation Filter:

▼ Description

The software constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component.

▼ Extended Description

This could allow attackers to execute unexpected, dangerous commands directly on the operating system. This weakness can lead to a vulnerability in environments in which the attacker does not have direct access to the operating system, such as in web applications. Alternately, if the weakness occurs in a privileged program, it could allow the attacker to specify commands that normally would not be accessible, or to call alternate commands with privileges that the attacker does not have. The problem is exacerbated if the compromised process does not follow the principle of least privilege, because the attacker-controlled commands may run with special system privileges that increases the amount of damage.

There are at least two subtypes of OS command injection:

1. The application intends to execute a single, fixed program that is under its own control. It intends to use externally-supplied inputs as arguments to that program. For example, the program might use `system("nslookup [HOSTNAME]")` to run nslookup and allow the user to supply a HOSTNAME, which is used as an argument. Attackers cannot prevent nslookup from executing. However, if the program does not remove command separators from the HOSTNAME argument, attackers could place the separators into the arguments, which allows them to execute their

High

▼ Demonstrative Examples

Example 1

This example code intends to take the name of a user and list the contents of that user's home directory. It is subject to the first variant of OS command injection.

Example Language: **PHP**

(bad code)

```
$userName = $_POST["user"];  
$command = 'ls -l /home/' . $userName;  
system($command);
```

The `$userName` variable is not checked for malicious input. An attacker could set the `$userName` variable to an arbitrary OS command such as:

```
;rm -rf /
```

(attack code)

Which would result in `$command` being:

```
ls -l /home/;rm -rf /
```

(result)

Since the semi-colon is a command separator in Unix, the OS would first execute the `ls` command, then the `rm` command, deleting the entire file system.

Also note that this example code is vulnerable to Path Traversal ([CWE-22](#)) and Untrusted Search Path ([CWE-426](#)) attacks.

Example 2

This example is a web application that intends to perform a DNS lookup of a user-supplied domain name. It is subject to the first variant of OS command injection.

The CWE Top 25

Below is a brief listing of the weaknesses in the 2019 CWE Top 25, including the overall score of each.

Rank	ID	Name	Score
[1]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
[3]	CWE-20	Improper Input Validation	43.61
[4]	CWE-200	Information Exposure	32.12
[5]	CWE-125	Out-of-bounds Read	26.53
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24.54
[7]	CWE-416	Use After Free	17.94
[8]	CWE-190	Integer Overflow or Wraparound	17.35
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	15.54
[10]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.10
[11]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.47
[12]	CWE-787	Out-of-bounds Write	11.08
[13]	CWE-287	Improper Authentication	10.78
[14]	CWE-476	NULL Pointer Dereference	9.74
[15]	CWE-732	Incorrect Permission Assignment for Critical Resource	6.33
[16]	CWE-434	Unrestricted Upload of File with Dangerous Type	5.50
[17]	CWE-611	Improper Restriction of XML External Entity Reference	5.48
[18]	CWE-94	Improper Control of Generation of Code ('Code Injection')	5.36
[19]	CWE-798	Use of Hard-coded Credentials	5.12
[20]	CWE-400	Uncontrolled Resource Consumption	5.04
[21]	CWE-772	Missing Release of Resource after Effective Lifetime	5.04
[22]	CWE-426	Untrusted Search Path	4.40

The CWE Top 25 with Scoring Metrics

The following table shows the 2019 CWE Top 25 with relevant scoring information, including the number of entries related to a particular CWE within the NVD data set, and the average CVSS score for each weakness.

Rank	ID	NVD Count	Avg CVSS	Overall Score
[1]	CWE-119	3545	8.045	75.56
[2]	CWE-79	3430	5.778	45.69
[3]	CWE-20	2360	7.242	43.61
[4]	CWE-200	2300	5.961	32.12
[5]	CWE-125	1428	7.270	26.53
[6]	CWE-89	977	9.129	24.54
[7]	CWE-416	799	8.374	17.94
[8]	CWE-190	867	7.679	17.35
[9]	CWE-352	693	8.365	15.54
[10]	CWE-22	759	7.275	14.10
[11]	CWE-78	486	8.707	11.47
[12]	CWE-787	510	8.169	11.08
[13]	CWE-287	495	8.188	10.78
[14]	CWE-476	572	6.834	9.74
[15]	CWE-732	334	7.393	6.33
[16]	CWE-434	239	8.549	5.50
[17]	CWE-611	262	7.949	5.48
[18]	CWE-94	230	8.637	5.36
[19]	CWE-798	215	8.782	5.12
[20]	CWE-400	288	6.980	5.04
[21]	CWE-772	304	6.714	5.04
[22]	CWE-426	215	7.222	4.10

PRODUCTS

Official Common Platform Enumeration (CPE) Dictionary

CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Below is the current official version of the CPE Product Dictionary. The dictionary provides an agreed upon list of official CPE names. The dictionary is provided in XML format and is available to the general public. Please check back frequently as the CPE Product Dictionary will continue to grow to include all past, present and future product releases. The CPE Dictionary is updated nightly when modifications or new names are added. Archived CPE dictionaries are available at <https://nvd.nist.gov/feeds/xml/cpe/dictionary/>.

As of December 2009, The National Vulnerability Database is now accepting contributions to the Official CPE Dictionary. Organizations interested in submitting CPE Names should contact the NVD CPE team at cpe_dictionary@nist.gov for help with the processing of their submission.

The CPE Dictionary hosted and maintained at NIST may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

CPE Dictionary

1. [Official CPE Dictionary v2.3, gz format](#) - 6.21MB, Updated:12/10/2019 12:45:12 AM EST
2. [Official CPE Dictionary v2.3, zip format](#) - 6.21MB, Updated:12/10/2019 12:45:12 AM EST
3. [Official CPE Dictionary v2.2, gz format](#) - 8.42MB, Updated:12/10/2019 12:45:12 AM EST
4. [Official CPE Dictionary v2.2, zip format](#) - 8.42MB, Updated:12/10/2019 12:45:12 AM EST

Q Search Results (Refine Search)

Search Parameters:

- Keyword: synology
- CPE Status: FINAL
- CPE Naming Format: 2.3

There are **1,003** matching records.

Displaying matches **181** through **200**.

<<	<	6	7	8	9	10	11	12	13	14	15
>	>>										

Vendor	Product	Version	Update	Edition	Language
cpe:2.3:a:synology:cloud_station_drive:4.2.8-4421:*:*:*:*:* <small>View CVEs</small>	synology	cloud_station_drive	4.2.8-	4421	
cpe:2.3:a:synology:cloud_station_drive:4.3.0-4435:*:*:*:*:* <small>View CVEs</small>	synology	cloud_station_drive	4.3.0-	4435	
cpe:2.3:a:synology:cloud_station_drive:4.3.1-4437:*:*:*:*:* <small>View CVEs</small>	synology	cloud_station_drive	4.3.1-	4437	
cpe:2.3:a:synology:diskstation_manager:-:*:*:*:*:* <small>View CVEs</small>	synology	diskstation_manager	-		
cpe:2.3:a:synology:diskstation_manager:3.0:*:*:*:*:* <small>View CVEs</small>	synology	diskstation_manager	3.0		
cpe:2.3:a:synology:diskstation_manager:4.0:*:*:*:*:* <small>View CVEs</small>	synology	diskstation_manager	4.0		
cpe:2.3:a:synology:diskstation_manager:4.0-2259:*:*:*:*:* <small>View CVEs</small>	synology	diskstation_manager	4.0-2259		

CPE Summary

[Return to Search Listing](#)

CPE Names

Version 2.3: `cpe:2.3:a:synology:diskstation_manager:6.2.2-24922:*:*:*:*:*`

Version 2.2: `cpe:/a:synology:diskstation_manager:6.2.2-24922`

[Read information about CPE Name encoding](#)



CPE NAME COMPONENTS SELECT A COMPONENT TO SEARCH FOR SIMILAR CPES

Part: a	Language:
Vendor: synology	Software Edition:
Product: diskstation_manager	Target Software:
Version: 6.2.2-24922	Target Hardware:
Update:	Other:
Edition:	

QUICK INFO

Created On: 05/09/2019
Last Modified On: 05/09/2019

Metadata

Titles: Text

Locale

Synology Diskstation Manager 6.2.2-24922

en_US

References:

Type	Description	URL
------	-------------	-----

+ Version

- * List vulnerable version

- 1.2.3

- 1.2.3, 2.3.1, and 3.1.2

+ Version

- * List vulnerable version
- * Earlier versions are affected
 - 1.2.3 and earlier
 - 1.2.3, 2.3.1, 3.1.2, and earlier

+ Version

- * List vulnerable version
- * Earlier versions are affected
- * Fixed or updated version
 - before 1.2.3
 - before 1.2.3, 2.x before 2.3.1, and 3.x before 3.1.2

+ Version

- * List vulnerable version
- * Earlier versions are affected
- * Fixed or updated version
- * **Vulnerable range**
 - 1.2.1 through 1.2.3
 - 1.2.1 through 1.2.3 and 2.0.1 through 2.3.1

9.8
(Critical)

Base Score

Attack Vector (AV)

Network (N)

Adjacent (A)

Local (L)

Physical (P)

Attack Complexity (AC)

Low (L)

High (H)

Privileges Required (PR)

None (N)

Low (L)

High (H)

User Interaction (UI)

None (N)

Required (R)

Scope (S)

Unchanged (U)

Changed (C)

Confidentiality (C)

None (N)

Low (L)

High (H)

Integrity (I)

None (N)

Low (L)

High (H)

Availability (A)

None (N)

Low (L)

High (H)

Vector String -

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

+ Attacker

- * Remote attackers
 - AV:N
- * Remote authenticated users
 - AC:L
- * Local users
 - PR:N
- * Physically proximate attackers
- * Man-in-the-middle attackers

+ Attacker

- * Remote attackers
 - * Remote authenticated users
 - * Local users
 - * Physically proximate attackers
 - * Man-in-the-middle attackers
- AV:N
 - AC:L
 - PR:L

+ Attacker

- * Remote attackers
- * Remote authenticated users
- * **Local users**
- * Physically proximate attackers
- * Man-in-the-middle attackers

- AV:L

- AC:L

- PR:L

+ Attacker

- * Remote attackers
 - * Remote authenticated users
 - * Local users
 - * **Physically proximate attackers**
 - * Man-in-the-middle attackers
- AV:P
 - AC:L
 - PR:N

+ Attacker

- * Remote attackers
 - AV:N
- * Remote authenticated users
 - AC:H
- * Local users
 - PR:N
- * Physically proximate attackers
- * **Man-in-the-middle attackers**

+ Attacker

- * Remote [TYPE] servers
- * Guest OS users
- * Guest OS administrators
- * Context-dependent attackers
- * [EXTENT] user-assisted [ATTACKER]
- * Attackers



About CAPEC

Objective

The Common Attack Pattern Enumeration and Classification (CAPEC™) effort provides a publicly available catalog of common attack patterns that helps users understand how adversaries exploit weaknesses in applications and other cyber-enabled capabilities.

"Attack Patterns" are descriptions of the common attributes and approaches employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. Attack patterns define the challenges that an adversary may face and how they go about solving it. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples.

Each attack pattern captures knowledge about how specific parts of an attack are designed and executed, and gives guidance on ways to mitigate the attack's effectiveness. Attack patterns help those developing applications, or administrating cyber-enabled capabilities to better understand the specific elements of an attack and how to stop them from succeeding.

Some Well-Known Attack Patterns:

- HTTP Response Splitting ([CAPEC-34](#))
- Session Fixation ([CAPEC-61](#))
- Cross Site Request Forgery ([CAPEC-62](#))
- SQL Injection ([CAPEC-66](#))
- Cross-Site Scripting ([CAPEC-63](#))
- Buffer Overflow ([CAPEC-100](#))



CAPEC-94: Man in the Middle Attack

Attack Pattern ID: 94

Abstraction: Meta

Status: Draft

Presentation Filter:

▼ Description

This type of attack targets the communication between two components (typically client and server). The attacker places himself in the communication channel between the two components. Whenever one component attempts to communicate with the other (data flow, authentication challenges, etc.), the data first goes to the attacker, who has the opportunity to observe or alter it, and it is then passed on to the other component as if it was never observed. This interposition is transparent leaving the two compromised components unaware of the potential corruption or leakage of their communications. The potential for Man-in-the-Middle attacks yields an implicit lack of trust in communication or identify between two components. MITM attacks differ from sniffing attacks since they often modify the communications prior to delivering it to the intended recipient. These attacks also differ from interception attacks since they may forward the sender's original unmodified data, after copying it, instead of keeping it for themselves.

▼ Likelihood Of Attack

High

▼ Typical Severity

Very High

▼ Relationships

The table below shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as ChildOf and ParentOf, and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as CanFollow, PeerOf, and CanAlsoBe are defined to show similar attack patterns that the user may want to explore.

Nature	Type	ID	Name
ParentOf		219	XML Routing Detour Attacks

Exchange public keys using a secure channel

▼ Example Instances

Leveraging security vulnerabilities and inherent functionality within web browsers, an adversary may be able to execute a "Man in the Browser" (MITB) attack. The initial compromise of this attack is generally a Trojan delivered to a victim's system via phishing attacks, drive-by malware installations, or malicious browser extensions. Once the Trojan is on the victim system, the adversary can observe and intercept traffic such as cookies, HTTP sessions, and SSL client certificate, which may allow for browser pivoting into an authenticated session. MITB attacks also circumvent common security mechanisms such as two and three factor authentication, as well as SSL/PKI.

For example, after installing a Trojan, an adversary positions himself between the victim and their banking institution. The victim begins by initiating a funds transfer from their personal savings to their personal checking account. Using injected JavaScript, the adversary captures this request and modifies it to transfer an increased amount of funds to an account that he controls, before sending it to the bank. The bank processes the transfer and sends the confirmation notice back to the victim, which is instead intercepted by the adversary. The adversary modifies the confirmation to reflect the original transaction details and sends this modified message back to the victim. Upon receiving the confirmation, the victim assumes the transfer was successful and is unaware that their money has just been transferred to the adversary.

▼ Related Weaknesses

A Related Weakness relationship associates a weakness with this attack pattern. Each association implies a weakness that must exist for a given attack to be successful. If multiple weaknesses are associated with the attack pattern, then any of the weaknesses (but not necessarily all) may be present for the attack to be successful. Each related weakness is identified by a CWE identifier.

CWE-ID	Weakness Name
300	Channel Accessible by Non-Endpoint ('Man-in-the-Middle')
290	Authentication Bypass by Spoofing
593	Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created
287	Improper Authentication
294	Authentication Bypass by Capture-replay
724	OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management

▼ Taxonomy Mappings

Relevant to the ATT&CK taxonomy mapping

Entry ID	Entry Name
1090	Connection Proxy
1185	Man in the Browser

The CERT Oracle
Secure Coding
Standard for Java
(2011)

SEC06-J

Do not rely on the default automatic signature verification provided by URLClassLoader and java.util.jar

▼ Related Attack Patterns

CAPEC-ID	Attack Pattern Name
CAPEC-117	Interception
CAPEC-466	Leveraging Active Man in the Middle Attacks to Bypass Same Origin Policy
CAPEC-57	Utilizing REST's Trust in the System Resource to Register Man in the Middle
CAPEC-589	DNS Blocking
CAPEC-590	IP Address Blocking
CAPEC-612	WiFi MAC Address Tracking
CAPEC-613	WiFi SSID Tracking
CAPEC-615	Evil Twin Wi-Fi Attack
CAPEC-94	Man in the Middle Attack

▼ References

[REF-244] M. Bishop. "Computer Security: Art and Science". Addison-Wesley. 2003.

► Content History

Page Last Updated: June 20, 2019



Use of the Common Weakness Enumeration and the associated references from this website are subject to the [Terms of Use](#). For more information, please email cwe@mitre.org.

CWE is sponsored by the [U.S. Department of Homeland Security](#) (DHS) [Cybersecurity and Infrastructure Security Agency](#) (CISA). Copyright © 2006-2019, The MITRE Corporation. CWE, CWSS, CWRAF, and the CWE logo are trademarks of [The MITRE Corporation](#).

[Privacy Policy](#)
[Terms of Use](#)
[Site Map](#)
[Contact Us](#)

```
... @@ -1,18 +1,80 @@
```

```
1 {
2 -   "data_type": "CVE",
3 -   "data_format": "MITRE",
4 -   "data_version": "4.0",
5   "CVE_data_meta": {
6     "ID": "CVE-2019-11820",
7 -   "ASSIGNER": "cve@mitre.org",
8 -   "STATE": "RESERVED"
```

```
9 },
```

```
1 {
2   "CVE_data_meta": {
3 +   "ASSIGNER": "security@synology.com",
4 +   "DATE_PUBLIC": "2019-05-09T00:00:00",
5     "ID": "CVE-2019-11820",
6 +   "STATE": "PUBLIC"
7 + },
8 + "affects": {
9 +   "vendor": {
10 +     "vendor_data": [
11 +       {
12 +         "product": {
13 +           "product_data": [
14 +             {
15 +               "product_name": "Calendar",
16 +               "version": {
17 +                 "version_data": [
18 +                   {
19 +                     "affected": "<",
20 +                     "version_value": "2.3.3-0620"
21 +                   }
22 +                 ]
23 +               }
24 +             }
25 +           ]
26 +         },
27 +         "vendor_name": "Synology"
28 +       }
29 +     ]
30 +   }
31 + }
```

```
31 },
```

```
32 + "data_format": "MITRE",
```

```
11     "description_data": [  
12         {  
13             "lang": "eng",  
14 -         "value": "** RESERVED ** This candidate has been reserved by an  
organization or individual that will use it when announcing a new security problem. When  
the candidate has been publicized, the details for this candidate will be provided."
```

```
36     "description_data": [  
37         {  
38             "lang": "eng",  
39 +         "value": "Information exposure through process environment vulnerability  
in Synology Calendar before 2.3.3-0620 allows local users to obtain credentials via  
cmdline."  
40 +         }  
41 +     ]  
42 + },  
43 +     "impact": {  
44 +         "cvss": {  
45 +             "attackComplexity": "LOW",  
46 +             "attackVector": "LOCAL",  
47 +             "availabilityImpact": "NONE",  
48 +             "baseScore": 5.5,  
49 +             "baseSeverity": "MEDIUM",  
50 +             "confidentialityImpact": "HIGH",  
51 +             "integrityImpact": "NONE",  
52 +             "privilegesRequired": "HIGH",  
53 +             "scope": "CHANGED",  
54 +             "userInteraction": "REQUIRED",  
55 +             "vectorString": "CVSS:3.0/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:N/A:N",  
56 +             "version": "3.0"  
57 +         }  
58 +     },  
59 +     "problemtype": {  
60 +         "problemtype_data": [  
61 +             {  
62 +                 "description": [  
63 +                     {  
64 +                         "lang": "eng",  
65 +                         "value": "Information Exposure Through Process Environment (CWE-  
214)"  
66 +                     }  
67 +                 ]  
68 +             }  
69 +         ]  
70 +     }
```

```

50 +         "confidentialityImpact": "HIGH",
51 +         "integrityImpact": "NONE",
52 +         "privilegesRequired": "HIGH",
53 +         "scope": "CHANGED",
54 +         "userInteraction": "REQUIRED",
55 +         "vectorString": "CVSS:3.0/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:N/A:N",
56 +         "version": "3.0"
57 +     }
58 + },
59 +     "problemtype": {
60 +         "problemtype_data": [
61 +             {
62 +                 "description": [
63 +                     {
64 +                         "lang": "eng",
65 +                         "value": "Information Exposure Through Process Environment (CWE-
214)"
66 +                     }
67 +                 ]
68 +             }
69 +         ]
70 +     },
71 +     "references": {
72 +         "reference_data": [
73 +             {
74 +                 "name": "https://www.synology.com/security/advisory/Synology_SA_19_21",
75 +                 "refsource": "CONFIRM",
76 +                 "url": "https://www.synology.com/security/advisory/Synology_SA_19_21"
77 +             }
78 +         ]
79 +     }
18 - }

```

💡 **ProTip!** Use `n` and `p` to navigate between commits in a pull request.

技術專欄



你用它上網，我用它進你內網! 中華電信數據機遠端代碼執行漏洞

DEVCORE CONF, CVE, RCE

By  Orange Tsai on 2019-11-11

Tree: 9f49009a43 ▾ cvelist / 2019 / 13xxx / CVE-2019-13411.json

Find file

Copy path

cve-team "-Synchronized-Data."

9f49009 on Oct 18

2 contributors  

97 lines (97 sloc) | 3.05 KB

Raw

Blame

History



```
1  {
2    "CVE_data_meta": {
3      "ASSIGNER": "cve@cert.org.tw",
4      "DATE_PUBLIC": "2019-10-16T16:00:00.000Z",
5      "ID": "CVE-2019-13411",
6      "STATE": "PUBLIC",
7      "TITLE": "A remote command execution vulnerability was discovered in HiNet GPON firmware < I040GWR190731 port 3097"
8    },
9    "affects": {
10     "vendor": {
11       "vendor_data": [
12         {
13           "vendor_name": "HiNET",
14           "product": {
15             "product_data": [
16               {
17                 "product_name": "GPON",
18                 "version": {
19                   "version_data": [
20                     {
21                       "version_value": "firmware before I040GWR190731"
22                     }
23                   ]
24                 }
25             ]
26           }
27         }
28       ]
29     }
30   }
31 }
```



```
1  {
2    "CVE_data_meta": {
3      "ASSIGNER": "cve@cert.org.tw",
4      "DATE_PUBLIC": "2019-10-16T16:00:00.000Z",
5      "ID": "CVE-2019-13411",
6      "STATE": "PUBLIC",
7      "TITLE": "A remote command execution vulnerability was discovered in HiNet GPON firmware < I040GWR190731 port 3097"
8    },
9    "affects": {
10     "vendor": {
11       "vendor_data": [
12         {
13           "vendor_name": "HiNET",
14           "product": {
15             "product_data": [
16               {
17                 "product_name": "GPON",
18                 "version": {
19                   "version_data": [
20                     {
21                       "version_value": "firmware before I040GWR190731"
22                     }
23                   ]
24                 }
25               }
26             ]
27           }
28         }
29       ]
30     }
31   },
32   "credit": [
33     {
34       "lang": "eng",
35       "value": "DEVCORE"
36     }
37   ]
38 }
```



```
33     {
34         "lang": "eng",
35         "value": "DEVCORE"
36     }
37 ],
38 "data_format": "MITRE",
39 "data_type": "CVE",
40 "data_version": "4.0",
41 "description": {
42     "description_data": [
43         {
44             "lang": "eng",
45             "value": "An \u201cinvalid command\u201d handler issue was discovered in HiNet GPON firmware < I040GWR190731. It allows an
46         }
47     ]
48 },
49 "generator": {
50     "engine": "Vulnogram 0.0.8"
51 },
52 "impact": {
53     "cvss": {
54         "attackComplexity": "LOW",
55         "attackVector": "NETWORK",
56         "availabilityImpact": "HIGH",
57         "baseScore": 10,
58         "baseSeverity": "CRITICAL",
59         "confidentialityImpact": "HIGH",
60         "integrityImpact": "HIGH",
61         "privilegesRequired": "NONE",
62         "scope": "CHANGED",
63         "userInteraction": "NONE",
64         "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
65         "version": "3.1"
66     }
67 },
68 "problemtype": {
69     "problemtype_data": [
70         {
71             "description": [
```

```
54     "attackComplexity": "LOW",
55     "attackVector": "NETWORK",
56     "availabilityImpact": "HIGH",
57     "baseScore": 10,
58     "baseSeverity": "CRITICAL",
59     "confidentialityImpact": "HIGH",
60     "integrityImpact": "HIGH",
61     "privilegesRequired": "NONE",
62     "scope": "CHANGED",
63     "userInteraction": "NONE",
64     "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
65     "version": "3.1"
66   }
67 },
68   "problemtype": {
69     "problemtype_data": [
70       {
71         "description": [
72           {
73             "lang": "eng",
74             "value": " execute arbitrary command"
75           }
76         ]
77       }
78     ]
79   },
80   "references": {
81     "reference_data": [
82       {
83         "name": "https://www.twcert.org.tw/en/cp-128-3013-92adb-2.html",
84         "refsource": "CONFIRM",
85         "url": "https://www.twcert.org.tw/en/cp-128-3013-92adb-2.html"
86       },
87       {
88         "name": "https://tvn.twcert.org.tw/taiwanvn/TVN-201908005",
89         "refsource": "CONFIRM",
90         "url": "https://tvn.twcert.org.tw/taiwanvn/TVN-201908005"
91       }
92     ]
93   }
94 }
```

```
69     "problemtyp_data": [  
70         {  
71             "description": [  
72                 {  
73                     "lang": "eng",  
74                     "value": " execute arbitrary command"  
75                 }  
76             ]  
77         }  
78     ]  
79 },  
80 "references": {  
81     "reference_data": [  
82         {  
83             "name": "https://www.twcert.org.tw/en/cp-128-3013-92adb-2.html",  
84             "refsource": "CONFIRM",  
85             "url": "https://www.twcert.org.tw/en/cp-128-3013-92adb-2.html"  
86         },  
87         {  
88             "name": "https://tvn.twcert.org.tw/taiwanvn/TVN-201908005",  
89             "refsource": "CONFIRM",  
90             "url": "https://tvn.twcert.org.tw/taiwanvn/TVN-201908005"  
91         }  
92     ]  
93 },  
94 "source": {  
95     "discovery": "UNKNOWN"  
96 }  
97 }
```



+ CVE-2019-13411 (TWCERT/CC)

An “invalid command” handler issue was discovered in HiNet GPON firmware < I040GWR190731.

It allows an attacker to execute arbitrary command through port 3097. CVSS 3.0 Base score 10.0.

CVSS vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

[VULNTYPE] in [COMPONENT] in
[VENDOR] [PRODUCT] [VERSION] allows
[ATTACKER] to [IMPACT] via [VECTOR].

+ CVE-2019-13411 (Revised)

OS command injection vulnerability in omcimain in HiNet GPON firmware before I040GWR190731 allows remote attackers to execute arbitrary command via port 3097.

+ Cross-site Scripting (1-1)

Cross-site scripting (XSS) vulnerability in [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] allows remote attackers to inject arbitrary web script or HTML via the [PARAM] parameter.

+ Cross-site Scripting (1-N)

Multiple cross-site scripting (XSS) vulnerabilities in [VENDOR] [PRODUCT] [VERSION] allow remote attackers to inject arbitrary web script or HTML via the [PARAM] parameter to (1) [COMPONENT₁], (2) [COMPONENT₂], ..., or (n) [COMPONENT_n].

+ Cross-site Scripting (N-1)

Multiple cross-site scripting (XSS) vulnerabilities in [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] allow remote attackers to inject arbitrary web script or HTML via the [PARAM₁], (2) [PARAM₂], ..., or (n) [PARAM_n] parameter.

+ Cross-site Scripting (N-N)

Multiple cross-site scripting (XSS) vulnerabilities in [VENDOR] [PRODUCT] [VERSION] allow remote attackers to inject arbitrary web script or HTML via the (1) [PARAM₁] or (2) [PARAM₂] parameter to [COMPONENT₁]; the (3) [PARAM₃] parameter to [COMPONENT₂]; ...; or (n) [PARAM_n] parameter to [COMPONENT_m].

+ SQL Injection (1-1)

SQL injection vulnerability in [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] allows [ATTACKER] to execute arbitrary SQL commands via the [PARAM] parameter.

+ SQL Injection (1-N)

Multiple SQL injection vulnerabilities in [VENDOR] [PRODUCT] [VERSION] allow [ATTACKER] to execute arbitrary SQL commands via the [PARAM] parameter to (1) [COMPONENT₁], (2) [COMPONENT₂], ..., or (n) [COMPONENT_n].

+ SQL Injection (N-1)

Multiple SQL injection vulnerabilities in [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] allow [ATTACKER] to execute arbitrary SQL commands via the (1) [PARAM₁], (2) [PARAM₂], ..., or (n) [PARAM_n] parameter.

+ SQL Injection (N-N)

Multiple SQL injection vulnerabilities in [VENDOR] [PRODUCT] [VERSION] allow [ATTACKER] to execute arbitrary SQL commands via the (1) [PARAM₁] or (2) [PARAM₂] parameter to [COMPONENT₁]; the (3) [PARAM₃] parameter to [COMPONENT₂]; ...; (n) [PARAM_n] parameter to [COMPONENT_m].

+ Counting Decisions

- * CNT1 | Independently Fixable
- * CNT2 | Vulnerability
 - CNT2.1 | Vendor Acknowledgment
 - CNT2.2A | Claim-Based
 - CNT2.2B | Security Model-Based

+ Counting Decisions

* CNT3

- Shared Codebase
- Libraries, Protocols, or Standards

+ Inclusion Decisions

- * INC1 | In Scope of Authority
- * INC2 | Intended to be Public
- * INC3 | Installable / Customer-Controlled Software
- * INC4 | Generally Available and Licensed Product
- * INC5 | Duplicate

+ Edge Cases

- * MD5 / SHA-1
- * Default Credentials
- * Cloudbleed
- * End-of-life products

+ Edge Cases

- * MD5 / SHA-1
- * **Default Credentials**
- * Cloudbleed
- * End-of-life products

+ Edge Cases

- * MD5 / SHA-1
- * Default Credentials
- * **Cloudbleed**
- * End-of-life products

+ Edge Cases

- * MD5 / SHA-1
- * Default Credentials
- * Cloudbleed
- * End-of-life products



VideoLAN ✓

@videolan

Official tweets from the #VideoLAN project, #VLC and the community.

videolan.org

videolan.org

Joined November 2009



VideoLAN ✓

@videolan

Follow

About the "security issue" on #VLC : VLC is not vulnerable.

tl;dr: the issue is in a 3rd party library, called libebml, which was fixed more than 16 months ago.

VLC since version 3.0.3 has the correct version shipped, and @MITREcorp did not even check their claim.

Thread:

2:41 AM - 24 Jul 2019

3,004 Retweets 4,047 Likes



72 3.0K 4.0K



VideoLAN ✓ @videolan · Jul 24

So, a reporter, opened a bug on our bugtracker, which is outside of the reporting policy, aka, mail us in private on the security alias.

Of course, our bugtracker is public.

We could not, of course reproduce the issue, and tried to contact the security researcher, in private.

Commits on Jul 26, 2019

"-Synchronized-Data."

 cve-team committed Jul 26, 2019

Verified



47f2177



"-Synchronized-Data."

 cve-team committed Jul 26, 2019

Verified



84107d2



Commits on Jul 25, 2019

"-Synchronized-Data."

 cve-team committed Jul 25, 2019

Verified



f62fd51



Commits on Jul 22, 2019

"-Synchronized-Data."

 cve-team committed Jul 22, 2019

Verified



7ecd6ea



Commits on Jul 17, 2019

"-Synchronized-Data."

 cve-team committed Jul 17, 2019

Verified



24f486c



```
84     }
85   ]
86 },
87 +     {
88 +       "refsource": "REDHAT",
89 +       "name": "RHSA-2019:1833",
90 +       "url": "https://access.redhat.com/errata/RHSA-2019:1833"
91     },

```

2 2019/13xxx/CVE-2019-13615.json

@@ -34,7 +34,7 @@

```
34     "description_data": [
35     {
36         "lang": "eng",
37 -         "value": "VideoLAN VLC media player 3.0.7.1 has a heap-based buffer over-
read in mkv::demux_sys_t::FreeUnused() in modules/demux/mkv/demux.cpp when called from
mkv::Open in modules/demux/mkv/mkv.cpp."
38     }
39     ]
40     },

```

56 2019/3xxx/CVE-2019-3485.json

@@ -1,17 +1,61 @@

```
1     {
2 +       "data_type": "CVE",
3 +       "data_format": "MITRE",
4 +       "data_version": "4.0",
5       "CVE_data_meta": {
6         "ID": "CVE-2019-3485",
7 +       "ASSIGNER": "security@suse.com",

```



```

@@ -34,7 +34,7 @@
34     "description_data": [
35     {
36         "lang": "eng",
37 -         "value": "VideoLAN VLC media player 3.0.7.1 has a heap-based buffer over-
read in mkv::demux_sys_t::FreeUnused() in modules/demux/mkv/demux.cpp when called from
mkv::Open in modules/demux/mkv/mkv.cpp. NOTE: It has been reported that the vulnerability
originates in libebml before 1.3.6 and was fixed in the 3.0.3 binary version of VLC."
38     }
39     ]
40 },

```

```

@@ -61,6 +61,21 @@

```

```

61     "refsource": "BID",
62     "name": "109304",
63     "url": "http://www.securityfocus.com/bid/109304"

```

```

34     "description_data": [
35     {
36         "lang": "eng",
37 +         "value": "libebml before 1.3.6, as used in the MKV module in VideoLAN VLC
Media Player binaries before 3.0.3, has a heap-based buffer over-read in
EbmlElement::FindNextElement."
38     }
39     ]
40 },

```

```

61     "refsource": "BID",
62     "name": "109304",
63     "url": "http://www.securityfocus.com/bid/109304"

```

```

64 +     },
65 +     {
66 +         "refsource": "MISC",
67 +         "name": "https://github.com/Matroska-
Org/libebml/commit/05beb69ba60acce09f73ed491bb76f332849c3a0",
68 +         "url": "https://github.com/Matroska-
Org/libebml/commit/05beb69ba60acce09f73ed491bb76f332849c3a0"
69 +     },
70 +     {
71 +         "refsource": "MISC",
72 +         "name": "https://github.com/Matroska-Org/libebml/compare/release-
1.3.5...release-1.3.6",
73 +         "url": "https://github.com/Matroska-Org/libebml/compare/release-
1.3.5...release-1.3.6"
74 +     },
75 +     {
76 +         "refsource": "UBUNTU",
77 +         "name": "USN-4073-1",
78 +         "url": "https://usn.ubuntu.com/4073-1/"

```

+ Update CVE Entries

* Reject

- Not a vulnerability (fails CNT2)
- Not to make the vulnerability public (fails INC2)
- Not customer controlled (fails INC3)
- Not generally available (fails INC4)

+ Update CVE Entries

- * Reject

- * Merge

- Not independently fixable (fails CNT1)
- Result of shared codebase, library, etc. (fails CNT3)
- Duplicate assignment (fails INC5)

+ Update CVE Entries

- * Reject

- * Merge

- * Split

- Contains interpedently fixable bugs (passes CNT1)
- Not share a codebase (fails CNT3)
- To be implementation specific (fails CNT3)

+ Update CVE Entries

- * Reject

- * Merge

- * Split

- * **Dispute**

- Validity of the vulnerability is questioned

+ Update CVE Entries

- * Reject

- * Merge



- * Split



- * Dispute


- * **Partial Duplicate**


- Editor
- Source
- Advisory
- MITRE-Preview
- CVE-JSON

CVEx_data_meta


 ID [MITRE](#) [NVD](#)  ASSIGNER


 DATE_PUBLIC  Also known as


 TITLE

 STATE PUBLIC RESERVED REJECT

source


 Defect

 Advisory-ID

 Found during internal research external research production use unknown

affects

vendor

vendor_name	product			
Synology	 product_name	Calendar		
	Version name (X)	version_affected	Version value (n)	platform
	eg., 4.0	Not Selected	2.3.3-0620	eg., x86
<div style="text-align: right;">affected <input type="text" value="string"/></div> <div style="text-align: right;"><</div>				
<input type="button" value="+ Add version"/>				
<input type="button" value="+ Add product"/>				

source

Defect CNA specific bug tracking IDs

Advisory-ID CNA specific advisory IDs (Optional)

Found during internal research external research production use unknown

affects

vendor

vendor_name	product			
Synology	product_name	Calendar		
	Version name (X)	version_affected	Version value (n)	platform
	eg., 4.0	Not Selected ▼	2.3.3-0620	eg., x86
affected string ▼				
<				
+ Add version				
+ Add product				
+ Add vendor				

problemtype

description

Information Exposure Through Process Environment (CWE-214)

+ Add problem type

description Auto-Text

Information exposure through process environment vulnerability in Synology Calendar before 2.3.3-0620 allows local users to obtain credentials via cmdline.

Synology	eg., 4.0	Not Selected	2.3.3-0620	eg., x86	<
----------	----------	--------------	------------	----------	---

+ Add version

+ Add product

+ Add vendor

 **problemtype**

description

Information Exposure Through Process Environment (CWE-214)

+ Add problem type

 **description** ✎ Auto-Text

Information exposure through process environment vulnerability in Synology Calendar before 2.3.3-0620 allows local users to obtain credentials via cmdline.

+ Add description

 **references**

refsource	url	name
CONFIRM	https://www.synology.com/security/advisory/Synology_SA_19_21	https://www.synology.com/security/advisory/Synology_SA_19_21

+ Add URL

 **configuration**

+ Add required configuration

 **impact**

Common Vulnerability Scoring System (CVSS) 3.1

Capture the principal characteristics of a vulnerability and produce a numerical score (zero to ten) reflecting its severity.

configuration

+ Add required configuration

impact

Common Vulnerability Scoring System (CVSS) 3.1

Capture the principal characteristics of a vulnerability and produce a numerical score (zero to ten) reflecting its severity.

attackVector PHYSICAL LOCAL ADJACENT_NETWORK NETWORK

attackComplexity HIGH LOW

privilegesRequired HIGH LOW NONE

userInteraction REQUIRED NONE

scope UNCHANGED CHANGED

confidentialityImpact NONE LOW HIGH

integrityImpact NONE LOW HIGH

availabilityImpact NONE LOW HIGH

vectorString CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:N/A:N

[Open in CVSS Calculator](#)

baseScore 5.5

baseSeverity MEDIUM

exploit

+ Add Exploit

work_around

+ Add work around

solution

+ Add solution

credit

+ Add vendor


problemtype

description

Information Exposure Through Process Environment (CWE-214)

+ Add problem type

 description

 Auto-Text

Information exposure through process environment vulnerability in Synology Calendar before 2.3.3-0620 allows local users to obtain credentials via cmdline.



Information Exposure Through Process Environment (CWE-214) vulnerability in ____COMPONENT____ of Synology Calendar allows ____ATTACKER/ATTACK____ to cause ____IMPACT____.




This issue affects:
Synology Calendar
2.3.3-0620.



+ Add description

references

refsource	url	name
CONFIRM ▼	https://www.synology.com/security/advisory/Synology_SA_19_21	https://www.synology.com/security/advisory/Synology_SA_19_21

 Open link

+ Add URL

+ Catch 'Em All

- * How CVE and CNA works

+ Catch 'Em All

- * How CVE and CNA works
- * Why Synology want to be a CNA
 - Expertise around products within our scope
 - Control the disclosure policy and procedure

+ Catch 'Em All

- * How CVE and CNA works
- * Why Synology want to be a CNA
- * How to write CVE descriptions
 - CWE / CPE
 - Version
 - Attacker

+ Catch 'Em All

- * How CVE and CNA works
- * Why Synology want to be a CNA
- * How to write CVE descriptions
- * **CVE counting rules**
 - Counting decisions
 - Inclusion decisions